From:
Dr. Nicholas Weaver, Ph.D.
International Computer Science Institute
2150 Shattuck Ave, Ste. 250,
Berkeley, CA 94704
nweaver@icsi.berkeley.edu

To:
The Honorable Lewis A. Kaplan
United States District Judge
Southern District of New York
Daniel Patrick Moynihan Courthouse
500 Pearl Street
New York, New York 10007-1312

Via ~~United States Postal Service Express Mail~~ UPS

Re: US v Bankman-Fried, (1:22-cr-00673)

Judge Kaplin

I am a lecturer in Computer Science at the University of California at Berkeley and a researcher at the International Computer Science Institute in Berkeley. I am writing this amicus letter as an individual and uninterested party in US vs Bankman-Fried (1:22-cr-00673) to offer an explanation of VPN technologies and usages as well as a comparison to a similarly situated defendant's bond conditions in a lower profile cryptocurrency case.

I received my Ph.D. in Computer Science from UC Berkeley in 2003 and have focused a considerable amount of my teaching and research on computer security in particular, both network security and cryptocurrency related issues. I also observe many cryptocurrency related court cases due to their public policy implications. My CV is available at https://www1.icsi.berkeley.edu/~nweaver/cv.html.

I hold no cryptocurrency, I have never met Mr Bankman-Fried, and have no financial interest in this case.

A Virtual Private Network, or VPN, is an internet "tunnel": it acts to route some or all of a user's network communication to a remote location. From this remote location the communication is then forwarded onto the open Internet or onto an internal network.

A VPN is an encrypted connection, so that anyone observing the network connection can only see that information is passing through the VPN but is unable to see the contents or metadata. The result is that the "source" of the traffic on the network becomes the other side of the VPN.

A VPN is primarily used for three separate purposes: access control to internal resources, bypassing geographic restrictions on content, and protection against local network monitoring.

Access Control: It is generally considered poor practice for internal business resources to be generally accessible to the Internet. Instead, these resources are protected by the "network firewall" which blocks all external requests. In order for an external authorized user to access these resources, the firewall allows external connections for the VPN tunnel. The user logs into the VPN and now their computer is considered "inside the network" for purposes of the internal resources.

Such VPN connections are usually run in a "split tunnel" model. If the user wants to access internal resources, their traffic is processed by the VPN. But all other user traffic is instead directly sent by the user's computer over the user's normal internet connection. This restriction can be enforced by the VPN tunnel, if the VPN tunnel refuses to route traffic on to the general Internet.

Bypassing Geographic Or Similar Restrictions: A significant amount of Internet content is limited to some geographic areas or networks. So, for example, a streaming service in Jamaica will attempt to limit external connections to computers in Jamaica. These restrictions are enforced by a "GeoIP database", a mapping of computer internet addresses to probable country locations, so the computer serving the content would look up where the computer is connecting from and check whether it is an allowed country.

Thus if someone wished to access this streaming service from outside the Bahamas they would pay for a Jamaican VPN service. When active, all the user's traffic would then appear to be coming from a computer located in Jamaica, so the streaming service would allow access.

A similar use often occurs for university students or faculty. They might use the campus VPN to route all their network traffic through the campus, allowing external websites, such as journal publications, to know that the user has a university affiliation.

Evading Local Network Monitoring: Since a VPN encrypts all traffic, this enables a user to evade local network monitoring and censorship. So, for example, a user in China may use a VPN to evade the Chinese "Great Firewall" censorship system and freely access outside information.

But a VPN's encrypted traffic is different from the encrypted traffic that is common on the web (everytime a site uses "https"). Web encryption hides the content of the traffic (so, for example, someone monitoring a user's connection can't see that user's Google searches) but does not hide the identity of the site a user connects to.

A VPN also hides "metadata" from anyone monitoring the network. Network metadata says what computers are talking, when, and how much data (e.g. network metadata can distinguish

between a connection to Google and a connection to a Mastodon instance and can see the volume transferred) but not the content of the communication.

This is important in the context of legal monitoring through a Pen Register/Trap-and-Trace (PR/TT) order on an Internet connection[1]. If a user does not use a VPN, the PR/TT effectively collects information about what sites the user visits, when, and how much data is transferred between the user and the site.

If the user uses a VPN, the only data the PR/TT is able to collect is "this user was not online at these times" (when the VPN tunnel is not sending traffic, as some VPNs may further add additional traffic even when the user isn't actually accessing the network).

I hope the previous discussion was helpful in understanding what a VPN is used for and why it may be of concern in this case.

One additional observation: Mr Bankman-Fried's terms of home detention are remarkably lenient for a cryptocurrency-related defendant with regard to Internet access. As an independent observer I was surprised that the initial terms of home confinement did not include a complete "no Internet" restriction.

An example of a lower profile but similarly situated defendant's terms were those of Larry Harmon (US v Larry Harmon, District of Columbia case 1:19-cr-00395) who's terms of home detention on a personal recognisance bond set by Judge Beryl A Howell included a complete restriction on using Internet connected devices (docket 20).

Larry Harmon was accused of running the "Grams" darknet market search engine and the "Helix" cryptocurrency mixer. There were natural concerns by the government that he could access otherwise unknown cryptocurrency assets and/or be a flight risk due to significant foreign connections (docket 16). These concerns appear to be identical in this case, as Mr Bankman-Fried likewise may have unknown assets and has significant foreign ties. There were no stated concerns by the government in the Harmon case concerning witness tampering.

Thank you for your time

Sincerely Yours
Nicholas Weaver, Ph.D.

2/18/2023

[1] The US government in their filings revealed that there is an existing PR/TT on Mr Bankman-Fried's Google account. Although they do not reveal that there is also a PR/TT order on Mr Bankman-Fried's internet connections, the legal standard for obtaining such an order is the same for both, strongly suggesting there is such an order already in place.